United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of:
A silver Chevrolet Cruze bearing Oklahoma license plate OK NQT830

FILED UNDER SEAL

Case No. 24-MJ-202-GLJ

APPLICATION FOR SEARCH WARRANT

I, Jessica Jennings, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the **EASTERN** District of **OKLAHOMA** *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A-3"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B-3"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation Title 18, United States Code, Section(s) 1151, 1152, 2241(c), 2422(b), 2252(a)(2) and (b)(1), and 2252(a)(4)(B) and (b)(2) and the application is based on these facts:

☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

JESSICA JENNINGS
Special Agent
Homeland Security Investigations

Sworn to :

Date: June 20, 2024

Judge's signature

City and state: Muskogee, Oklahoma

GERALD L. JACKSON
UNITED STATES MAGISTRATE JUDGE
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of 601 N Ash St, Sallisaw OK, the person of Michael Blaine HARRIS, and A silver Chevrolet Cruze bearing Oklahoma license plate OK NQT830	**Case No. _____** **FILED UNDER SEAL**

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, Jessica Jennings, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for three separate search warrants for the person and location specifically described in Attachment A of this affidavit, including:

a. Search Warrant 1: the entire property located at 601 N Ash St., Sallisaw, Sequoyah County, Eastern District of Oklahoma, including outbuildings and vehicles on the curtilage premises ("Subject Residence");

b. Search Warrant 2: the person of Michael Blaine HARRIS, Date of Birth: [xx/xx/1993] ("HARRIS"); and

c. Search Warrant 3: a silver Chevrolet Cruze vehicle bearing OK NQT830; and the content of electronic storage devices located therein;

for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2241(c) (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2422(b) (Coercion or

Enticement of a Minor), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), which items are more specifically described in Attachment B of this affidavit.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations (HSI) in Tulsa, Oklahoma, since July 2022. I am a graduate of the Criminal Investigator Training Program and the Homeland Security Investigations Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21, and 31 of the United States Code (U.S.C.). I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

4. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation, including the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the areas of child pornography and child

exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

5. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

6. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1151, 1152, and 2241(c) (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), will be located at 601 N. Ash Street, Sallisaw, OK 74955, Sequoyah County, Eastern District of Oklahoma, including outbuildings and vehicles on the curtilage premises, and on the person of Michael Blaine HARRIS, as further described in Attachment A.

Jurisdiction

7. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

8. The requested search is related to the following violations of federal law:

a. 18 U.S.C. §§ 2241(c) (Aggravated Sexual Abuse of a Minor) which states: Whoever crosses a State line with intent to engage in a sexual act with a person who has not attained the age of 12 years, or in the special maritime and territorial jurisdiction of the United States or in a Federal prison, or in any prison, institution, or facility in which persons are held in custody by direction of or pursuant to a contract or agreement with the head of any Federal department or agency, knowingly engages in a sexual act with another person who has not attained the age of 12 years, or knowingly engages in a sexual act under the circumstances described in subsections (a) and (b) with another person who has attained the age of 12 years but has not attained the age of 16 years (and is at least 4 years younger than the person so engaging), or attempts to do so, shall be fined under this title and imprisoned for not less than 30 years or for life. If the defendant has previously been convicted of another Federal offense under this subsection, or of a State offense that would have been an offense under either such provision had the offense occurred in a Federal prison, unless the death penalty is imposed, the defendant shall be sentenced to life in prison.

b. 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor) which states: Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

c. 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) which states: Any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if—(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct shall be punished as provided in subsection (b) of this section.

d. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) which states: Any person who knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct shall be punished as provided in subsection (b) of this section.

Definitions

9. The following definitions, inclusive of all definitions contained in 18 U.S.C. §§ 2246 and 2256, apply to this affidavit and the attachments incorporated herein:

a. the term "sexual act" means—

contact between the penis and the vulva or the penis and the anus, and for purposes of this subparagraph contact involving the penis occurs upon penetration, however slight;

contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus;

the penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person; or

the intentional touching, not through the clothing, of the genitalia of another person who has not attained the age of 16 years with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person;

b. the term "serious bodily injury" means bodily injury that involves a substantial risk of death, unconsciousness, extreme physical pain, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental faculty;

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

d. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;

e. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's

computer a particular IP address that is used each time the computer accesses the Internet;

f. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most commons methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

g. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

h. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade,

photographic, mechanical, electrical, electronic, or magnetic form;

k. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and

l. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Background on Digital Media Storage Devices

10. The ability of a computer (including a smartphone) to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Given the storage capabilities, modern computers can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered. Other digital media storage devices (e.g., compact disks, digital video disks, thumb drives, etc.) can also store tremendous amounts of digital information, including digital video and picture files.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of

one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Further, even if deleted, forensic examination can sometimes recover files and data including deleted picture files. I know that computers such as laptops, iPhones, and other smartphones can be forensically examined, and forensic analysts can learn much detail about the user's habits and online activities, including websites visited, files downloaded, Google searches performed, locations where the device was used, dominion and control information, etc.

12. Computers and other digital file storage devices can store the equivalent of thousands of pages of digital information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires the searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks depending on the volume of the data stored, and it would be generally impossible to accomplish this kind of data search on site. Furthermore, I know that smartphones (a type of "computer," as broadly defined in 18 U.S.C. § 1030(e)(1))

like an iPhone can typically "synch" with a traditional desktop or laptop computer. The purpose of synching a smartphone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smartphone is lost or damaged. Also, smartphone users may move files off the smartphone and onto a computer to free up storage space on the smartphone. Similarly, computer (e.g., desktop computers, smartphones, etc.) users may move files off of one computer onto another computer or digital file storage devices such as a thumb drive, a DVD, an external hard drive to free up space on the computer. For this reason, I am seeking authorization to seize and search all computers and digital file storage devices at the Subject Residence, Vehicle, and/or on the Person of HARRIS—not any particular computer.

Probable Cause

13. In April 2024, Special Agents from Homeland Security Investigations (HSI) Tulsa Office received information regarding a 14-year-old minor victim (MV) from Tulsa Police Department. The MV resides in Catoosa, Oklahoma, in the Northern District of Oklahoma. MV is a registered member of the Cherokee Nation Tribe.

14. On April 10, 2024, HSI Special Agent Jennings received multiple reports from Tulsa Police Department Detective Paula Maker. One of those reports details a forensic interview of MV. The following details are contained in that report or are from my review of the forensic interview recording.

15. On March 18, 2024, MV was forensically interviewed at the Children's

Advocacy Center. MV revealed that she met up with a subject she knows as "Blaine" and that he is in his thirties. Regarding her interactions with HARRIS, MV stated the following:

a. MV said that she met him on Anti and that "Blaine" told her he was purposely looking for minors. MV told "Blaine" she was 14 years old when he asked.

b. MV stated "Blaine" picked her up and dropped her off in a silver small boxy car.

c. MV stated they went to a parking lot the first time and "he fingered my vagina". MV stated "Blaine" was too paranoid to get hard and that he spoke dirty talk to her.

d. MV stated that "Blaine" lived two hours away, close to the Arkansas border.

e. MV stated that they met three times. The other two times she met him they went to a hotel behind an O'Reilly's in Catoosa. She said they had sex and took a shower together. When they got to hotel, "he put his penis in me". She stated that he did not use protection.

f. MV stated that the first time at the hotel, "Blaine" tied her hands behind her back and took a picture of her naked on the bed. He used his phone to take the picture. She believed he had a Samsung phone.

g. MV stated that she sent "Blaine" pictures/videos of herself masturbating. "Blaine" saved those pictures in his camera roll. She talked to Blaine in

Anti and Snapchat.

h. The forensic interviewer asked MV what "sex" means to her. MV said when he penetrates her vagina with his penis.

16. I received information from Tulsa Police Department Detective Maker that MV disclosed a Facebook page of "Blaine Harris" to MV's mother. MV's mother provided that information to Detective Maker. Detective Maker showed MV the Facebook page for "Blaine Harris" and various images of "Blaine Harris" to MV from that Facebook page. MV confirmed the images as the subject that had sexual intercourse with her. MV's mother additionally provided Detective Maker with information that Blaine told the MV he lives in an apartment in Sallisaw, Oklahoma. Facebook photographs of the profile for "Blaine Harris" provided by Detective Maker appear visually similar to the Oklahoma Driver's License photographs of Michael Blaine HARRIS.

17. I received additional information from Tulsa Police Department Detective Maker. Detective Maker revealed that the hotel in question, in which MV stated that she had sex with "Blaine," would be Catoosa Inn and Suites, 40 S. 193rd Street, Room 103, Tulsa, Oklahoma 74108 and the date would be January 8, 2024.

18. On May 6, 2024, I served an administrative subpoena to Catoosa Inn and Suites for a booking by Name(s): Michael Blaine Harris, Michael Harris, Blaine Harris with Known Booking(s): 01/08/2024 for Room 103. On May 6, 2024, an employee of the hotel provided me with an invoice for Michael HARRIS on January 8, 2024 for Room 103. The invoice shows that a payment of $78.79 was paid with a

Visa. There is a guest signature on the page.

19. On June 12, 2024, I received additional information from Catoosa Inn & Suites regarding the booking for Michael Harris on January 8, 2024. Catoosa Inn and Suites provided the following information for Room 103, Day In January 8, 2024 and Day Out January 9, 2024:

a. Name: Michael Blaine Harris

b. Address: 601 N Ash St, Sallisaw, OK 749552407, USA

c. Phone # 580-729-0946

d. ID Type: Driver License

e. ID #: M0XXXXXX39

f. Issue Place: Sallisaw

20. A records check shows that the address of Michael Blaine HARRIS's driver's license is 601 N. Ash Street, Sallisaw, OK. 601 N. Ash Street appears to be a duplex residence. On May 21, 2024, Steven Jenkins of Sequoyah County Sheriff's Office conducted surveillance of 601 N. Ash Street, Sallisaw, Oklahoma. On that date at approximately 1505 hours, he observed a single vehicle at the residence bearing Oklahoma license plate NQT830.

21. A records check of that plate reveals that it comes back to a 2014 silver Chevrolet Cruze to Michael B HARRIS at 601 N. Ash Street, Sallisaw, OK.

22. A record check was performed with the Cherokee Nation, and MV is an enrolled member of the Cherokee Nation, with some degree of Indian blood.

Characteristics Common to Individuals who Exhibit a Sexual Interest in Children and Individuals who Distribute, Receive, Possess and/or Access with Intent to View Child Pornography

23. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or

some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child

pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"[1] it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Michael Blaine HARRIS uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the Subject Residence, Vehicle, and/or the person of Michael Blaine HARRIS, as set forth in Attachment A.

Background on Child Pornography, Computers, and the Internet

24. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, smartphones[2] and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers

[2] Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are

plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by

saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Systems

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Residence, Vehicle and/or the person of Michael Blaine HARRIS in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. I submit that if a computer or storage medium is found on the Subject Residence, Vehicle and/or the person of Michael Blaine HARRIS, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file;

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information;

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Residence, Vehicle and/or the person of Michael Blaine HARRIS because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified;

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed

networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it

is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to

conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a

password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

29. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging

information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

BACKGROUND ON DNA AS A FORM OF EVIDENCE

31. Deoxyribonucleic acid (DNA) is a genetic material which has become widely accepted as one of the most reliable ways of identifying an individual person based on DNA found in many bodily substances including but not limited to blood, semen, skin cells, and saliva. If a DNA-containing substance is located at a crime scene or is otherwise collected, proper collection and analysis of this substance may produce a viable "DNA profile" from the collected sample with which to then compare a "known sample," or DNA that was known to be collected from a specific

person. If the collected sample's DNA profile is compared with a known sample's DNA profile, it may be determined whether the two come from the same source (same person) within a given degree of probability.

COLLECTION OF A KNOWN DNA SAMPLE FROM A PERSON

32. The collection of a known DNA sample from a person for the purposes of this criminal investigation will be performed using a buccal swab. The buccal swab typically consists of a handle with a tip made of a type of foam or other material. The buccal swab comes in a sterile wrapper to prevent contamination from outside materials. Use of the buccal swab involves swabbing the inside of a person's cheeks for several seconds, resulting in a collection of biological material containing DNA, while ensuring the swab is not contaminated by other materials. The buccal swab is then placed in a package which protects it from contamination. The buccal swab process is minimally invasive to the person from whom the sample is taken.

Conclusion

33. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. § 2241(c) (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View

Child Pornography) has been violated, and that the contraband, property, evidence, fruits and instrumentalities of this offense, more fully described in Attachment B, are located at the sites described in Attachment A. I respectfully request that this Court issue search warrants for the locations described in Attachment A, authorizing the search and seizure of the items described in Attachment B.

34. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

Jessica Jennings
Special Agent
Homeland Security Investigations

Sworn to [by phone] on June 20, 2024.

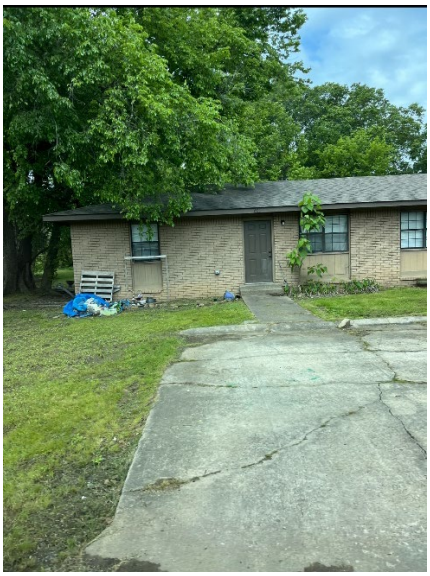
GERALD L. JACKSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to be Searched

The property to be searched is a multi-family residence located at 601 N. Ash Street, Sallisaw, Sequoyah County, Eastern District of Oklahoma, including outbuildings and vehicles on the curtilage premises, further described as a residence that appears to have tan brick. The residence has brown trim around the top. The front door of the residence is brown and faces east. The residence appears to be a duplex with 601 being the south portion of the dwelling. The numbers "601" are visible above the door.

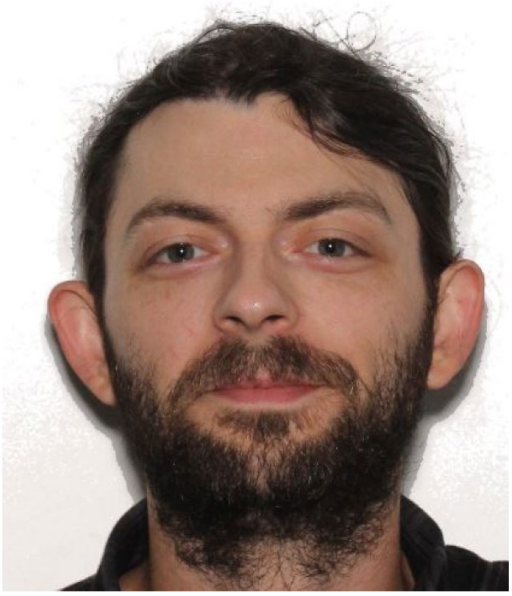
The premises to be searched is located within the Eastern District of Oklahoma, described above, and pictured below:



ATTACHMENT A-2

Property to be Searched

This warrant applies to the person of Michael Blaine HARRIS, date of birth XX/XX/1993, who is listed on his/her driver's license as 5'07 tall, weighing 130 pounds and hazel eyes, and who is pictured below:



ATTACHMENT A-3

Property to be Searched

A silver Chevrolet Cruze bearing Oklahoma license plate OK NQT830.

ATTACHMENT B-1

Particular Things to be Seized

All items that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1151, 1153, and 2241(c) (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2422(b) (enticement or coercion, or the attempt thereof, of a minor to engage in sexual activity by means of interstate commerce), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) involving Michael Blaine HARRIS, including:

a. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found including, but not limited to:

b. Any cellular telephone, smartphone, tablet, personal digital assistant, digital cameras, external storage devices, and any electronic data storage devices including, but not limited to flash memory devices, and other storage mediums related to or used to: visually depict child pornography; contain information

pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography; or relating to the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;]

i. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any

input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children; and

iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children];

c. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining

to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children];

iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and

acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors or a sexual interest in children];

iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors or a sexual interest in children;

v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums]

vi. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs];

vii. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

viii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

ix. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software];

d. Credit card information including, but not limited to, bills and payment records, and including, but not limited to, records of internet access;

e. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

f. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

g. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

h. Any data or materials establishing ownership, use or control of any computer equipment seized from 601 N. Ash Street, Sallisaw, OK 74955.

i. Any and all information, correspondence (including emails and text messages), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts.

j. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

k. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

l. The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM

cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

ATTACHMENT B-2

Particular Things to be Seized

All items that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1151, 1153, and 2241(c) (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2422(b) (enticement or coercion, or the attempt thereof, of a minor to engage in sexual activity by means of interstate commerce), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) involving Michael Blaine HARRIS, including:

a. The deoxyribonucleic acid (DNA) of **Michael Blaine HARRIS**, collected via buccal (cheek) swab and suitable for laboratory comparison;

b. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found including, but not limited to:

i. Any cellular telephone, smartphone, tablet, personal digital assistant, digital cameras, external storage devices, and any

electronic data storage devices including, but not limited to flash memory devices, and other storage mediums related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography; or relating to the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;]

ii. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film,

slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

iii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iv. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. §

2256 or relating to the sexual exploitation of minors or a sexual interest in children; and

v. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children];

c. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or

relating to the sexual exploitation of minors or a sexual interest in children;

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children];

iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors or a sexual interest in children];

iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors or a sexual interest in children;

v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums]

vi. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs];

vii. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

viii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

ix. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software];

d. Credit card information including, but not limited to, bills and payment records, and including, but not limited to, records of internet access;

e. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

f. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

g. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

h. Any data or materials establishing ownership, use or control of any computer equipment seized from 601 N. Ash Street, Sallisaw, Oklahoma 74955.

i. Any and all information, correspondence (including emails and text messages), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts.

j. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

k. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

l. The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

ATTACHMENT B-3

Particular Things to be Seized

All items that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1151, 1153, and 2241(c) (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2422(b) (enticement or coercion, or the attempt thereof, of a minor to engage in sexual activity by means of interstate commerce), 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) involving Michael Blaine HARRIS, including:

a. Proof of ownership of the vehicle described in Attachment A;

b. Receipts and documents relating to travel on dates mentioned by victim;

c. Personal documents, passports, and other identifying documents located in the vehicle;

d. Writings or other documents related to HARRIS's state of mind or intent to commit the crime;

e. Writings or other documents related to HARRIS's relationship with the victim of the crime; and

f. Electronic devices such as computers, cell phones, or storage media used to commit or facilitate the violation described above;

g. DNA evidence from vehicle, such as hair samples, fluid samples, or other forms of DNA that tie HARRIS to the victim of the crime.